



IT Security Handbook

Audit and Accountability

ITS Handbook (ITS-HBK-2810.16-01)
Audit and Accountability

Distribution:

NODIS

Approved

Valarie Burks

Valarie Burks
Deputy Chief Information Officer for
Information Technology Security

May 6, 20

Date

Change History

| Version | Date | Change Description |
|---------|------|--------------------|
| 1.0 | | Initial Draft |
| | | |
| | | |
| | | |
| | | |

Table of Contents

| | |
|---|-----|
| Change History | 3 - |
| 1 Introduction and Background | 5 - |
| 2 Auditable Events (AU-2)..... | 5 - |
| 3 Content of Audit Records (AU-3) | 6 - |
| 4 Audit Storage Capacity (AU-4) | 7 - |
| 5 Response to Audit Processing Failures (AU-5)..... | 7 - |
| 6 Audit Review, Analysis, and Reporting (AU-6)..... | 7 - |
| 7 Audit Reduction and Report Generation (AU-7)..... | 7 - |
| 8 Time Stamps (AU-8) | 7 - |
| 9 Protection of Audit Information (AU-9)..... | 7 - |
| 10 Non-Repudiation (AU-10) | 7 - |
| 11 Audit Record Retention (AU-11) | 7 - |
| 12 Audit Generation (AU-12) | 8 - |
| 13 Organizationally Defined Values..... | 9 - |

1 Introduction and Background

- 1.1 - NASA requirements for protecting the security of NASA information and information systems are derived from National Institute of Standards and Technology (NIST) guidance. Information System Owners (ISOs) and other personnel responsible for the protection of NASA information or information systems shall follow NIST guidance in the proper security categorization (*Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization for Federal Information and Information Systems*), and in the selection and implementation of information security controls (*FIPS 200, Minimum Security Requirements for Federal Information and Information Systems* and *NIST Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems and Organizations*), in a manner consistent with the Risk Management Framework (*NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems*).
- 1.2 - This handbook augments NIST guidance by providing NASA-specific requirements, procedures and recommendations, where applicable. NASA-specific guidance does not negate NIST guidance, unless explicitly stated.
- 1.3 - *NASA Policy Directive (NPD) 2810.1, NASA Information Security Policy, NASA Procedural Requirements (NPR) 2810.1, Security of Information Technology*, and the collection of 2810 Information Technology Handbooks (ITS-HBK) satisfy the policy and procedure controls of *NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations*.
- 1.1 - *NPR 2810.1, Security of Information Technology*, designates this handbook as a guide of NASA's Audit and Accountability (AU) information security controls.
- 1.2 - The terms "shall" and "may" within this handbook are used as defined in *ITS-HBK-0001, Format and Procedures for IT Security Policies and Handbooks*.
- 1.3 - The Audit and Accountability control family relates to the documentation and management of events that occur on or to information system components. Generally, the controls help to answer the questions of "who," "what," "where," "when," and sometimes "how" revolving around various types of information system activities and events (i.e., who logged into a given machine, when, and from where, etc.?). Such audit trails are used for individual accountability, intrusion detection, and problem identification. Such details are stored in logs which are used to produce useful, actionable information by applying data analysis techniques to detect anomalous trends and patterns that may be cause for concern. The logs can be used both retroactively to determine the causes of an adverse event, and proactively to detect and take action to avert an imminent adverse event.
- 1.4 - **Applicable Documents**
- *NPD 2810.1, NASA Information Security Policy*
 - *NITR 2810-19, Audit and Accountability Policy and Procedures*
 - *NPR 1441.1, NASA Records and Retention Schedule*
 - *NPR 2810.1, Security of Information Technology*
 - *ITS-HBK-0001, Format and Procedures for IT Security Policies and Handbooks*
 - *FIPS 199, Standards for Security Categorization for Federal Information and Information Systems*
 - *FIPS 200, Minimum Security Requirements for Federal Information and Information Systems*
 - *NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems*
 - *NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations*
 - *NIST SP 800-92, Guide to Computer Security Log Management*

2 Auditable Events (AU-2)

- 2.1 - **Roles and Responsibilities**
- 2.1.1 - *The Information System Owner (ISO) shall:*
- 2.1.1.1 Ensure the capability to audit the auditable events detailed by Table 1.
 - 2.1.1.2 Ensure the capability to automatically report audit information.

- 2.1.2 *The Information System Security Officer (ISSO) shall:*
 - 2.1.2.1 Identify those auditable events which may best inform after-the-fact investigative efforts.
 - 2.1.2.1.1 The frequency of auditing should be identified.
 - 2.1.2.2 Adjust as necessary, the frequency of audit activities.

Table 1 Auditable Events

| Event ID | Auditable Events | Event Description |
|----------|--|--|
| 1 | Audit Account Logon Event | Generates an event for credential validation. The event occurs on the computer that is authoritative for the credentials. For domain accounts, the domain controller is authoritative, and for local accounts, the local computer is authoritative. |
| 2 | Audit Account Management | Audits when a user account or group is created, changed, or deleted; a user account is renamed, disabled, or enabled; a password is set or changed. |
| 3 | Audit Directory Service Access | Audits the event of a user accessing an active directory object that has its own System Access Control List (SACL) specified. This setting is not applicable to Windows XP systems. |
| 4 | Audit Logon Events | Generates an event that records the creation and destruction of logon sessions. These events occur on the accessed computer. For interactive logons, these events are generated on the computer that is logged on to. For a network logon, such as access to a share, these events are generated on the computer that hosts the accessed resource. |
| 5 | Audit Object Access | Audits a user accessing an object (for example, a file, folder, registry key, or printer) that has its own SACL specified. Auditing of success or failure of system wide object access will create numerous log entries. Certain object access failures may be normal as a result of applications requesting all access types to objects, even though the application does not require all access types to function properly. Use object access auditing with caution. |
| 6 | Audit Policy Change | Audits every change to user rights assignment policies, audit policies, and trust policies. |
| 7 | Audit Privilege Use | Audits each instance of a user exercising a user right. This is likely to generate a very large number of events. |
| 8 | Audit of Process Tracking | Audits detailed tracking information for events such as program activation, process exit, handle duplication, and indirect object access. Enabling this setting will generate many events, so it should only be used when absolutely necessary. |
| 9 | Audit System Events | Audits events when a user restarts or shuts down the computer or when an event occurs that affects either the system security or the security log. |
| 10 | Audit the access of global system objects | Controls the ability to audit access of global systems objects. When this setting is enabled, system objects such as mutexes, events, semaphores, and DOS devices are created with a default system access control list (SACL). |
| 11 | Audit the use of Backup and Restore privilege | Controls the ability to audit the use of all user privileges, including Backup and Restore. If this policy is disabled, certain user rights will not be audited even if "Audit privilege use" audit policy is enabled. |
| 12 | User Data Persistence - Internet Zone - Local Computer | This policy setting supports preservation of information in the browser's history, in favorites, in an XML store, or directly within a Web page saved to disk. |
| 13 | User Data Persistence - Restricted Sites Zone - Local Computer | This policy setting supports the preservation of information in the browser's history, in favorites, in an XML store, or directly within a Web page saved to disk. |

3 Content of Audit Records (AU-3)

3.1 Roles and Responsibilities

- 3.1.1 *The ISSO shall:*
 - 3.1.1.1 Ensure that system audit records provide sufficient information to understand the details of recorded events.
 - 3.1.1.1.1 Information should include:
 - 3.1.1.1.1.1 Date and time of occurrence;
 - 3.1.1.1.1.2 Affected system component;
 - 3.1.1.1.1.3 Type of event;
 - 3.1.1.1.1.4 Affected user(s); and
 - 3.1.1.1.1.5 Outcome.

4 Audit Storage Capacity (AU-4)

- 4.1 - NIST guidance is the authoritative source for selection and implementation of this control based on the security categorization and risk environment of the information and/or information system. -

5 Response to Audit Processing Failures (AU-5)

5.1 - Roles and Responsibilities

5.1.1 - *The ISO shall:* -

- 5.1.1.1 - Ensure the capability of an information system to automatically notify designated officials in the case of impending or actual audit processing failures in a manner consistent with organizationally defined values. -

6 Audit Review, Analysis, and Reporting (AU-6)

6.1 - Roles and Responsibilities

6.1.1 - *The ISO shall:* -

- 6.1.1.1 - Ensure the review of audit records for unusual or suspicious activity in a manner consistent with organizationally defined values. -
 - 6.1.1.1.1 - Reviews should include system logs of activities of users with respect to the enforcement of information system access controls. -
 - 6.1.1.1.2 - The frequency of reviews should reflect the risk associated with the information system. -
- 6.1.1.2 - Report unusual or suspicious activities or violations as security incidents to the SOC. -

7 Audit Reduction and Report Generation (AU-7)

- 7.1 - NIST guidance is the authoritative source for selection and implementation of this control based on the security categorization and risk environment of the information and/or information system. -

8 Time Stamps (AU-8)

8.1 - Roles and Responsibilities

8.1.1 - *The ISO shall:* -

- 8.1.1.1 - Ensure that the capability exists to automatically synchronize the internal clocks of information system components in a manner consistent with organizationally defined values. -

9 Protection of Audit Information (AU-9)

9.1 - Roles and Responsibilities

9.1.1 - *The Senior Agency Information Security Officer (SAISO) shall:* -

- 9.1.1.1 - Ensure the availability of an Agency-wide repository for auditable event information. -
- 9.1.1.2 - Ensure the provision of sufficient resources for Agency-wide audit record management. -

9.1.2 - *The ISO shall:* -

- 9.1.2.1 - Ensure sufficient storage capacity resources for the archival of audit records. -

10 Non-Repudiation (AU-10)

10.1 - Roles and Responsibilities

10.1.1 - *The ISO shall:* -

- 10.1.1.1 - Ensure that digital signatures are validated using cryptographic schemes in a manner consistent with organizationally defined values. -

11 Audit Record Retention (AU-11)

11.1 - Roles and Responsibilities

- 11.1.1 *The ISO shall:*
 - 11.1.1.1 Ensure the archival of audit records in a manner consistent with organizationally defined values and, *NPR 1441.1.*

12 Audit Generation (AU-12)

12.1 Roles and Responsibilities

- 12.1.1 *The ISO shall:*
 - 12.1.1.1 Ensure the capability to generate audits for information system components in a manner consistent with organizationally defined values.

13 Organizationally Defined Values

The following table provides the values defined in *NIST SP 800-53* as being at the discretion of the implementing organization. The Section, and Parameter columns are intended to help navigate various *NIST SP 800-53* security controls for easier application of the organizationally defined values; these columns are defined as follows:

- Section: Values in this column indicate whether an organizationally defined value is in the main body of the control (Main), or part of one of the control's enhancements (E1, E2, etc).
- Parameter: Sometimes, a specific Section may have multiple organizationally defined values. In those instances, the bracketed number Parameters indicate which organizationally defined value (numbered sequentially) is being referenced. In the case of nested organizationally defined values, a series of bracketed numbers is used.

| Family | # | Name | Section | Parameter | Type | Description | Low | Moderate | High |
|--------|----|--|---------|-----------|------------|---|---|--|--|
| AU | 01 | Audit and Accountability Policy and Procedures | Main | [1] | Frequency | Policy and procedure review. | 1/Year | 1/Year | 1/Year |
| AU | 02 | Auditable Events | Main | [1] | Reference | List of auditable events. | See Table 1 ITS-HBK-2810.16-01 | See Table 1 ITS-HBK-2810.16-01 | See Table 1 ITS-HBK-2810.16-01 |
| AU | 02 | Auditable Events | Main | [2] | Reference | Subset of identified auditable events along with frequency of auditing. | ISO (Information System Owner) defined with rationale to support after-the-fact security incident investigation | ISO defined with rationale to support after-the-fact security incident investigation | ISO defined with rationale to support after-the-fact security incident investigation |
| AU | 02 | Auditable Events | E 3 | [1] | Frequency | Review and update of list of auditable events. | 1/Year | 1/Year | 1/Year |
| AU | 03 | Content of Audit Records | E 2 | [1] | Reference | Audit records are centrally managed if produced by: | | | ISO-Defined Devices. |
| AU | 05 | Response to Audit Processing Failures | Main | [1] | Reference | Additional actions taken in the event of an audit processing failure. | Overwrite oldest audit record. | Overwrite oldest audit record. | Overwrite oldest audit record. |
| AU | 05 | Response to Audit Processing Failures | E 1 | [1] | Percentage | Storage capacity warning threshold. | | | 80% |

ITS Handbook (ITS-HBK-2810.16-01) -
Audit and Accountability -

| Family | # | Name | Section | Parameter | Type | Description | Low | Moderate | High |
|--------|----|---------------------------------------|---------|-----------|-----------|--|----------------|---|---|
| AU | 05 | Response to Audit Processing Failures | E 2 | [1] | Reference | Audit failure events requiring real-time alerts. | | | 1. Hardware system failure or errors. 2. Software failures of errors. 3. Audit storage capacity exceeded. 4. System backup storage exceeded. |
| AU | 06 | Audit Review, Analysis, and Reporting | Main | [1] | Frequency | Review and analysis of audit records. | 1/60-Days | 1/30-Days | 1/30-Days |
| AU | 08 | Time Stamps | E 1 | [1] | Frequency | Synchronization of internal system clocks. | | 1/Day | 1/Day |
| AU | 08 | Time Stamps | E 1 | [2] | Reference | Authoritative time source. | | Coordinated Universal Time (UTC) via a NASA-controlled time source (e.g., the NISN NTP servers (preferred), a NASA IRIG-B feed, or an organizationally-owned and maintained GPS/CDMA NTP server appliance.); Other more accurate time services, as necessary. | Coordinated Universal Time (UTC) via a NASA-controlled time source (e.g., the NISN NTP servers (preferred), a NASA IRIG-B feed, or an organizationally-owned and maintained GPS/CDMA NTP server appliance.); Other more accurate time services, as necessary. |
| AU | 10 | Non-Repudiation | E 5 | [1] | Selection | Digital signature cryptography | FIPS-Validated | FIPS-Validated | FIPS-Validated |

ITS Handbook (ITS-HBK-2810.16-01) -
Audit and Accountability -

| Family | # | Name | Section | Parameter | Type | Description | Low | Moderate | High |
|--------|----|------------------------|---------|-----------|-------------|---|---|---|---|
| AU | 11 | Audit Record Retention | Main | [1] | Time Period | Audit record retention. | 1 Year | 1 Year | 1 Year |
| AU | 12 | Audit Generation | Main | [1] | Reference | Components with audit record generation capabilities. | 1. Servers 2. Workstations 3. Storage Devices/systems 4. Intrusion Detection Systems (IDS) and devices 5. Network devices | 1. Servers 2. Workstations 3. Storage Devices/systems 4. Intrusion Detection Systems (IDS) and devices 5. Network devices | 1. Servers 2. Workstations 3. Storage Devices/systems 4. Intrusion Detection Systems (IDS) and devices 5. Network devices |
| AU | 12 | Audit Generation | E 1 | [1] | Reference | Components with audit records that are compiled into system-wide audit trails. | | | 1. Servers 2. Workstations 3. Storage Devices/systems 4. Intrusion Detection Systems (IDS) and devices 5. Network devices |
| AU | 12 | Audit Generation | E 1 | [2] | Reference | Level of tolerance for relationship between time stamps of individual records in the audit trail. | | | 1 Second |